STATE OF NEVADA
GAMING CONTROL BOARD
MINIMUM INTERNAL CONTROL STANDARDS

INFORMATION TECHNOLOGY

General Controls

The standards in this subsection and the following subsection, "User Controls", must be addressed in detail in each applicable section, including the entertainment section, of the written system of internal control.

1. The main computers (i.e., hardware, software and data files) for each gaming application (e.g., keno, race and sports, slots, cashless wagering systems, etc.) and each application for entertainment and Regulation 6A are in a secured area with access restricted to authorized persons, including vendors.

2. Gaming and food/beverage personnel are precluded from having unrestricted access to the secured computer areas.

3. The computer systems, including application software, are secured through the use of passwords, biometrics, or other means approved by the Board.

4. Management personnel, or persons independent of the department being controlled, assign and control access to system functions to ensure adequate segregation of duties.

5. Adequate backup and recovery procedures are in place and, if applicable, include:

   a. Daily backup of data files.

      Note: This standard only applies if data files have been updated.

   b. Backup of all in-house developed and purchased software programs. Backup of purchased software is not required if the software can be reinstalled by the vendor.

   c. Secured storage of all backup data files and software programs, or other adequate protection to prevent the permanent loss of any data.

      Note 1: Backup data files and programs can be stored in a secured manner in another building on the premises that is physically separated from the building where the system's hardware and software are located. They may also be stored in the same building as the hardware/software as long as they are secured in a fireproof safe or some other manner that will ensure the safety of the files and programs in the event of a fire or other disaster.

      Note 2: MICS #5(c) does not apply to backup data files for computerized keno systems.

   d. Maintenance of a written plan outlining procedures for restoring data and program files.

      Note: While not mandatory, licensees are encouraged to test recovery procedures at least annually.

   e. For data files that are used in place of printed reports, quarterly testing of backup files is performed on a sample basis to ensure that the files are properly maintained.

6. Adequate system documentation is maintained, including descriptions of both hardware and software (including version numbers), operator manuals, etc.

User Controls

7. User identification numbers/names and passwords are controlled as follows unless otherwise addressed in these standards:

a. When multiple identification numbers/names per application are used, only one number may be active at a time and the user name has a unique prefix/suffix to easily identify the users with multiple operator numbers.

b. At least quarterly, personnel independent of the system functions under review perform verification procedures, by using the personnel access listing, to ensure that each employee's assigned system functions are being used as authorized, the assigned functions provide an adequate segregation of duties, and to determine whether terminated employees do not have access to system functions.

c. Generic identifications (user names) are prohibited unless user access is restricted to inquiry only functions.

d. Passwords are changed at least quarterly with changes documented. Documentation is not required if the system prompts users to change passwords and then denies access if the change is not completed.

e. The system is updated to change the status of terminated employees from active to inactive status within 72 hours of termination.

Note: It is recommended that inactive user identifications for IT Department employees are deleted from the system immediately upon termination.

8. System exception information (e.g., changes to system parameters, corrections, overrides, voids, etc.) is maintained.

9. Personnel access listings are maintained which include at a minimum:

a. Employee name and title or position.

b. Employee identification.

c. Listing of functions the employee can perform or equivalent means of identifying same.

Note: This listing may be archived daily in lieu of printing.

Information Technology Department

If a separate IT department is maintained or if there are in-house developed systems, MICS #10 through #13 are applicable.

10. The IT department is independent of the gaming operations (e.g., cage, pit, count rooms, etc.) and operations that are subject to entertainment tax.

11. IT department personnel are precluded from unauthorized access to:

a. Computers and terminals located in gaming areas.

b. Source documents (e.g., slot jackpot forms, table games fill/credit forms, wagering instruments).

c. Live data files (not test data).

12. New programs and program changes for in-house developed systems are documented as follows:

INFORMATION TECHNOLOGY

a. Requests for new programs or program changes are reviewed by the IT supervisory personnel. Approvals to begin work on the program are documented.

b. A written plan of implementation for new and modified programs is maintained and includes, at a minimum, the date the program is to be placed into service, the nature of the change (if applicable), a description of procedures required in order to bring the new or modified program into service (conversion or input of data, installation procedures, etc.), and an indication of who is to perform all such procedures.

c. Testing of new and modified programs is performed and documented prior to implementation.

d. A record of the final program or program changes, including evidence of user acceptance, date in service, programmer, and reason for changes, is documented and maintained.

e. A copy of the associated equipment reporting form submitted to the Board pursuant to Regulation 14 for each new program or program change, and a record that such software was approved for use is maintained.

Note: If only verbal approval is given, the notation of such approval is acceptable.

13. Computer security logs, if capable of being generated by the system, are reviewed by IT supervisory personnel for evidence of:

a. Multiple attempts to log-on. Alternatively, the system will deny user access after three attempts to log-on.

b. Changes to live data files.

c. Any other unusual transactions.

Note: This standard does not apply to personal computers.

Purchased Software Programs

14. New programs and program changes for purchased systems are documented as follows:

a. Documentation is maintained and includes, at a minimum, the date the program was placed into service, the nature of the change (if applicable), a description of procedures required in order to bring the new or modified program into service (conversion or input of data, installation procedures, etc.), and an indication of who performed all such procedures.

b. A copy of the associated equipment reporting form submitted to the Board pursuant to Regulation 14 for each new program or program change, and a record that such software was approved for use is maintained.

Note: If only verbal approval is given, the notation of such approval is acceptable.

c. Testing of new and modified programs is performed (by the licensee or the system manufacturer) and documented prior to full implementation.

Remote Access to Hardware and Software

15. For each computerized gaming or entertainment application that can be accessed remotely, the written system of internal control must specifically address remote access procedures including, at a minimum:

a. Type of gaming application, vendor's name and business address and version number, if applicable.

b. For cashless wagering systems only, the approved secured connection used so that the system can only be accessed from the vendor's place of business.

c. The procedures used in establishing and using passwords to allow authorized vendor personnel to access the system through remote access.

d. The personnel involved and procedures performed to enable the physical connection to the system when the vendor requires access to the system through remote access.

e. The personnel involved and procedures performed to ensure the physical connection is disabled when the remote access is not in use.

f. Any additional requirements relating to remote access published by the Board.

16. In the event of remote access, prepare a complete record of the access to include: name or identifier of end user's employee authorizing access, name or identifier of manufacturer's employee accessing system, description of work performed, date, time, and duration of access. The description of work performed must be adequately detailed to include the old and new version numbers of any software that was modified, and details regarding any other changes made to the system.

Computer Media Document Storage

17. Documents may be scanned or directly stored to unalterable media with the following conditions:

a. The storage media must contain the exact duplicate of the original document.

b. All documents stored must be maintained with a detailed index containing the casino department and date in accordance with Regulation 6.040(1). This index must be available upon Board request.

c. Upon request by Board agents, hardware (terminal, printer, etc.) must be provided in order to perform audit procedures.

d. Controls must exist to ensure the accurate reproduction of records, up to and including the printing of stored documents used for audit purposes.

e. At least quarterly, accounting/audit personnel review a sample of the documents on the storage media to ensure the clarity and completeness of the stored documents.

18. If source documents and summary reports are stored on re-writeable storage media, the media may not be relied upon for the performance of any audit procedures, and the original documents and summary reports must be retained.

Creation of Wagering Instruments Database

Note: MICS #19 - #22 apply when creating a database of wagering instruments that will be accepted by a cashless wagering system.

19. An individual independent of the gaming area performs the database creation and, if applicable, the creation of wagering instruments to be accepted in the cashless wagering system.

INFORMATION TECHNOLOGY

20. A record is maintained detailing the database creation and the wagering instruments to be accepted by the cashless wagering system, including evidence of user acceptance, date in service, and personnel involved.

21. Monthly, the wagering instrument database is reviewed and tested by personnel of the applicable gaming area and accounting/audit personnel for any improprieties.

22. The procedures used and subsequent results relating to the wagering instruments database review and test are documented and maintained.